Firewall Fundamentals

مقدمة :

تعريف بسيط : ال Firewall هو عبارة جهاز(Hardware) أو نظام(Software) يقوم بالتحكم عن في مسيرة ومرور البيانات في الشبكة أو بين الشبكات و التحكم يكون إما بالمنع أو السماح.غالبا يستخدم عند وجود الإنترنت و التعامل مع الـ TCP/IP protocol ولكن لايشترط ذلك .

قبل أن نتكلم بتفصيل عن الجدران النارية يجب أن أنذكر بعض صفاته ، و ماذا يستطيع أن يفعل الجدار الناري ؟ ...

- ✓ إن الجدار الناري يعتبر النقطة الفاصلة اللتي تبقى الغير الغير مصرح لهم بدخول الشكبة الخاصة من الدخول لها و التعامل معها بشكل مباشر و اللتي تقلل من إستغلال ثغرات هذه الشبكةو خدماتها كال , Ipspooing Routing Attacks .
- ✓ يحدد الجدار الناري إتجاه البيانات الصادرة و الواردة من و إلى الشبكة .
- ✓ يحدد الجدار الناري الأنظمة الموثوقة أو (Trusted System) و هو الجهاز أو الشبكة أو نظام التشغيل الموثوق بهم و اللتي يُسمح لها بالتعامل مع الشبكة الداخلية المحمية.
- ✓ يقوم الجدار الناري بمراقبة البيانات العابرة من و إلى الشبكة وأيضا تسجيل الأحداث و تتبعها و التنبيه عن أي أخطار أو أحداث غريبة تحصل .
- ✓ يقدم الجدار الناري موثوقيه التعامل مع بعض بروتوكلات الإنترنت و يقوم بعمل أشياء أخرى تخدم مستخدمين الشبكة المتصلين بالإنترنت كتوفير العنوانين (NAT) ، و أيضا يستطيع أن يعمل كذاكرة للمواقع اللتي تم زيارتها من قبل لتسريع الوصول لها فيما بعد لكامل الشبكة (Chash) .
- ✓ يخدم الجدار الناري أيضا سبل الإتصال الأمن المتعددة مثل IPsec و VPN .

و الأن سنذكر لن نقول عيوب بل الصحيح هو ، ما اللذي لا يستطيع أن يفعله الجدار الناري ؟ ...

- ✓ لا يستطيع الجدار الناري الحماية ضد الهجمات اللتي تعبر من الفايروول نفسه و اللتي تعتمد على ثغرات في بروتوكولات لا تستطيع الشبكة الاستغناء عنها .
- ✓ لا يستطيع الجدار الناري المخاطرة اللتي داخل الشبكة نفسها من الأفراد اللذي هم بطبيعة الحال داخل الشبكة و قد حصلوا على تلك الثقة اللتي جعلتهم في داخل الشبكة المحمية .
- ✓ لا يستطيع الجدار الناري الحماية من الفايروسات و الديدان في الشبكة و اللتي تشنتشر بسرعة و تسبب الخطورة على كامل الشبكه الداخليه حيث تنتقل عبر الرسائل و مشاركة الملفات و بعض الملفات الخبيثة المزروعة .

- ▪ خصائص الجدار الناري (Firewall Characteristics) :

سنقسم شرح خصائص الجدار الناري إلي قسمين لتوضيح فكرة الجدار الناري في العمل :

- i. أهداف تصميم الفايروول
- ii. التقنيات اللتي يستخدمها الفايروول في التحكم

i. أهداف تصميم الفايروول :

1- كل البيانات الداخلة و الخارجة من و إلى (كارت الشبكة – على مستوى الجهاز الواحد- أو على الشبكة – على مستوى شبكة -) يجب أن تمر بالجدار الناري أولا قبل الإنتقال للطرف الأخر .

2- يكون التحكم في البيانات عن طريق استثنائها أو استئصالها من المرور من و إلى الشبكه و متطلبات الشبكة و اللتي يراها مدير الشبكة هي اللتي تحدد تلك القواعد .

-3

ii. التقنيات اللتي يستخدمها الفايروول في التحكم

يستخدم الفايروول أربع أنواع للتحكم بالموصول إلى الشبكه و اللتي يسمى حينها Access Control و اللتي يستخدم غالبا طريقة التحكم في الخدمات اللتي تسمح بالوصول للشبكه للتحكم بالوصول من و إلى الشبكة ولكن هذه ليست الطريقة الوحيدة وسنذكر الطرق الأخرى و هي ..

- ✓ Service Control :

يحدد الفايروول أنواع خدمات الإنترنت و اللتي تستطيع عن طريقها الوصول من و إلى الشبكة (Inbound , Outbound) . قد يقوم الفايروول باستثناء أو استئصال البيانات العابرة سواء الخارج أو الداخلة بالإعتماد على IP address و أيضا ب TCP/UDP ports و ذلك بإجبار أجهزة الشبكة باتباعهم بروكسي (البروكسي هو عنوان الفايروول سيرفر و اللذي توجد فيه قواعد مرور و حجب الخدمات أو المواقع و غيرها) حيث بدونه لن تستطيع الحصول على الإنترنت مثلا.

- ✓ Detection Control :

يحدد الفايروول هنا لإتجاه الخدمات العابرة من و إلى الشبكة و اللتي يتحكم بها عن طريق السماح بالطلبات و تلبيتها و بهذا يحدد إتجاه الخدمات المستثناة و المستأصلة .

- ✓ User Control :

يحدد الفايروول هنا المستخدمين اللذين يسمح لهم بالوصول لمكان معين بوضع اسم مستخدم و كلمة مرور خاص لهم و يحدد لهم إستخدامهم لخدمات معينه وغالبا تطبق على المستخدمين اللذين هم داخل الشبكة مثل أن يسمح باستخدام الVPN أو IPsec و غيرها .

- ✓ Behavior Control :

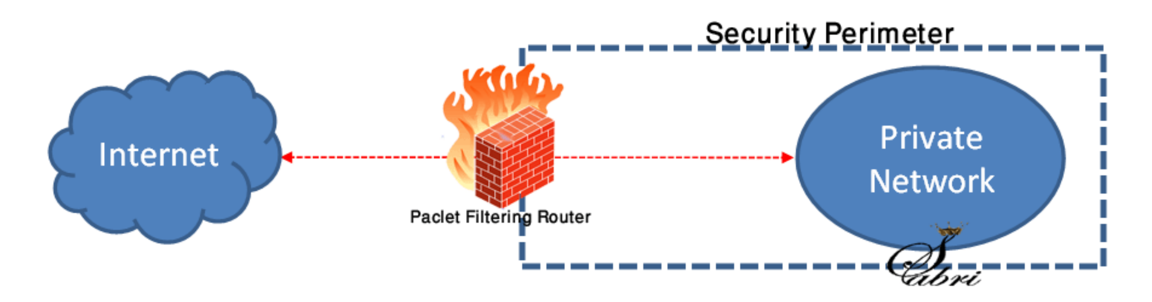
هنا يحدد سلوك استخدام خدمه معينة بطريقة معينة . مثال : أن لا يسمح لعملية الـping أو لبروتوكول ICMP بالتكرار أكثر من أربع مرات و تكون حجم حزمة البيانات لا تزيل عن165 كيلو بايت من نفس ال IP مثلا .. أو أنه يمنع رسائل السبام من الوصول إلى ال Mail server و هكذا .

- **<u>أنواع الجدران النارية (Types of Firewalls)</u>** :

هناك ثلاثة أنواع للجدران النارية سنوضحها بالرسم و الشرح بعد سردها سردا عاديا ..

i. Packet-Filters Router
ii. Application-Level Gateway
iii. Circuit-Level Gateway

i. Packet-Filters Router



عبارة عن مجموعة من القواعد (Roles) توضع للبيانات الواردة (incoming PKTs) و الصادرة (outgoing PKTs) حيث هي اللتي تحدد قرار البيانات إما بالتمرير أم الطرد أو التجاهل ، وسنذكر سبب هذه التسمية بتفصيل معنى كلمات الإسم نفسه لتعرفوا سبب التسمية

Router .. سمي بذلك لأنه طريقة عمله **شبيهة** بطريقة الراوتير في تمرير و رفض البيانات على الإتجاهين الصادر و الوارد (من و إلى الشبكة الداخلية) .

Packet-Filter .. قد يفهم أغلبنا أن الفلترة تعني الإستإصال على الإطلاق لكن الصحيح في الفلتره هي إما الاستئصال أو الاستثناء ، فالاستئصال يعني السماح للكل و منع البعض ، أنا الاستثناء فيعني منع الكل و السماح للبعض و طبعا كلتا الحالتين يجب أن تطبق عليها القواعد Roles الموضوعه من مدير الشبكة .

يكون تحديد المنع و السماح لجهاز معين أو لشبكة معينة بالطرق التالية :

- ✓ Source IP address : أي عنوان الجهاز أو الشبكة **المنتجة (المرسِل)** لحزمة البيانات نفسها و اللتي تقوم بإرسالها لجهاز أو شبكة أخرى .
- ✓ Destination IP address : أي عنوان الجهاز أو الشبكة **المستقبلة(المرسَل إليه)** لحزمة البيانات اللتي تم إرسالها من جهاز أو شبكة أخرى بغض النظر عن عنوان المرسل.
- ✓ Source and Destination Transport-Level address : وهنا في الحقيقة يعتم على منافذ البروتوكولات في تحديد قواعده مثل TCP/UDP ports numbers و اللتي ينتج عنها التحكم في التطبيقات المارة من و إلى الشبكة مثل Telnet , http , SMTP .
- ✓ IP protocol field : و هنا يعتمد في تحديده على البروتوكولات اللتي تعمل في Transport Layer .
- ✓ Interface : و هنا يعتمد على كارت/كروت الشبكة المتصل بالجهاز/الشبكة و يحدد ما يمر منها و إليها في قواعده .

o ملاحظة :

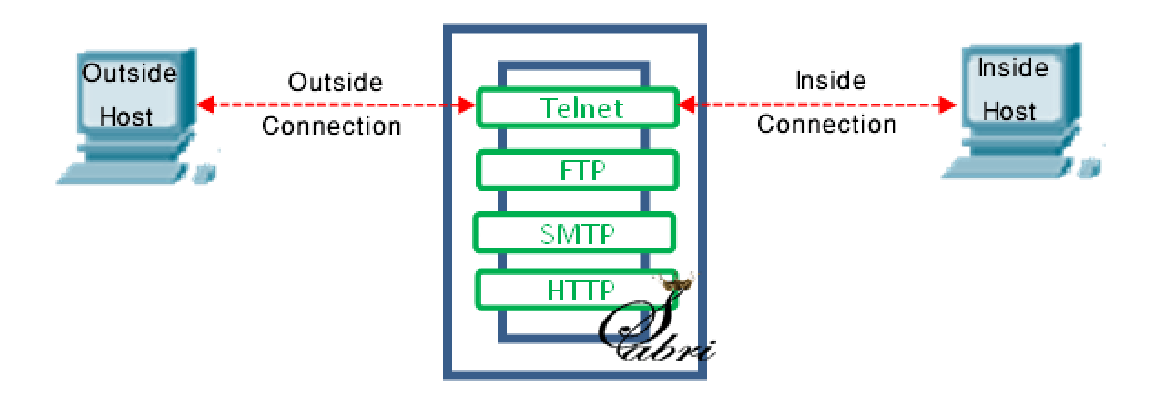
- إن أول قاعدة ثابتة تكون في جميع الجدران النارية هي قاعدة إفتراضية هي (إمنع الجميع) (Everything is Blocked) حيث هذه القاعدة هي الأكثر أمانا على الشبكة و من ثم يقوم مدير الشبكة بالسماح فقط لما يريد.
- إن القواعد تطبق في الجدار الناري من الأعلى إلي الأسفل حيث القاعدة الأحدث هي الأعلى أي هي من ستطبق أولا.
- لا فائدة من تطبيق نفس القاعدة مرتين .
- غالبا تكون القواعد الدنيا أقل صرامة من اللتي فوقها وليس شرطا

⇓ نقاط الضعف في نوع Packet Filter Firewall :

- بسبب أن الجدران النارية لا تنظر إلى البيانات المتبادلة في الطبقات العليا في OSI Layers فهي لا تستطيع منع الطبيقات اللتي تستغل ثغرات التطبيقات اللتي تعمل في هذه الطبقة ، مثل أن الجدار الناري لا يستطيع أن يمنع أوامر محددة و اللتي تصدر إلي النظام إذا كان يسمح بنوع اتصال يسمح باستقبال الأوامر مثلا إذا كان يسمح بالـ Telnet, SSH فلا يستطيع الفايروول أن يتحكم بالأوامر نفسها حيث أنه بعد السماح له لا ينظر ماذا يمرر من بيانات (أوامر)

- بسبب أن الفايروول لا يستطيع الحصول إلا على معلومات محدودة ، فإن تحكمه بالوصول يكون تقليدي جدا و محدود حيث كمان قلنا أنه يعتمد على (source add. , destination , traffic type)
- هناك ثغرات خطيرة في البروتوكلات اللتي لا غنى عنها و اللتي غالبا يجب السماح لها و اللتي تعمل في الطبقى الثالثة (Network Layer) و اللتي تعمد فيها هذه الثغرات على عمليات الـ Spoofing مثل (Routing , Addressing)
- من السهل جدا حدوث خطأ في وضع إعدادات (قواعد) الفايروول حيث يسمح لعناوين و خدمات يجب أن لا يسمح لها بالوصول إلي الشبكة او التعامل معها خلافا لقواعد الحماية المطلوبة في هذه الشبكة .

ii. Application-Level Gateway



أو ما يسمى بالـ *__Proxy Server__* حيث يعمل كمظم للطبة السابعة من OSI (Application Level) ، حيث يخرج المستخدم للعالم الخارجي عن طريق الـGateway باستخدام تطبيقات TCP/IP مثل Telnet , FTP حيث Gateway تسأل المستخدم اللذي يريد الإتصال عن اسم المستخدم و كلمة المرور للمصادقة لكي يتم إكتمال الاتصال و حينما تتطابق بالصواب فإن الإتصال يتم فإذا كانت الخدمة لم يتم تعريفها في ال Proxy server فإن الإتصال أو الخدمة المطلوبو لن يتم إتمامها و من هذه الخاصية فإن مدير الشبكة يستطيع بالسماح فقط للخدمات اللتي يريد تداولها و استخدامها و منع البقية كلها . يميز هذه الطريقة هو أنها تسمح بمراقبة و تسجيل كل ما يحصل في كل التطبقات العليا و السفلى .

⇓ نقاط الضعف في نوع Application Level Gateway :

- إن أكبر و أخطر نقطة ضعف في هذا النوع هو أنه يعمل عمليات معاجة أكثر بكثير من سابقة و أنه يحمل السيرفر حملا زائدا مما يؤثر على كفائته عن زيادة الضغط عليه حيث يقوم بفحص كل التطبيقات و مراكبتها الصادر منها و الوارد حيث يراقب اتصال ال end-to-end TCP .

iii. Circuit-Level Gateway

هذا النوع الثالث من أنواع الفايروول و اللذي تعمد فكرته على أنه يعمل كبوابة عبور Gateway ولكن تكون في __حالة تأهب__ لا تعمل مثل النوع الثاني (Application Level Gateway) حيث الأخير يضل يعمل و يراقب الإتصال حتى بعد السماح بالإتصال ، أما هذا النوع يعتمد في عمله على أنه عندما يقوم طرف بطلب الإتصال بطرف الأخر – لنفرض أن جهاز من داخل الشبكة أراد الإتصال بجهاز من خارج الشبكة – فإن هذا النوع يقوم بفتح إتصال بينه و بين الجهاز اللذي من داخل الشبكة ، ثم يقوم الفايروول بنفسه بإنشاء إتصال بينه و بين الجهاز اللذي من خارج الشبكة ثم بعد ذلك يتم توصيلهما ببعضهما و يترك الإتصال حرا لهما دون الإضطلاع على البيانات المرسلة داخل هذا النوع من الإتصال و يكون تلبية حاجة الحماية هنا عن طريق النظر إلي القواعد – هل تسمح بالاتصال أم لا – فإن كانت تسمح فإنه يتم الاتصال بنجاح و يترك لهما الإتصال براحة تامة .

ملاحظة :

- إن استخدام هذا النوع من الفايروول يستخدم من مدير الشبكة عندما يكون هناك ثقة بينه و بين مستخدمين الشبكة *__الداخلية__* .

- يستطيع هذا النوع العمل أيضا كـ *Proxy Server* **<u>للشبكة الداخلية</u>** و *Circuit-Level Gateway* **<u>للشبكة الخارجية</u>** . بهذه الطيرقة يكون قد قلل الحمل على السيرفر و مراقبة لكل الإتصالات و الطلبات.

- إن من أشهر و أقوى الأمثلة على Circuit-Level Gateway هو الـ **<u>SOCKS</u>**

ما هو الـ SOCKS ؟

هو بروتوكول وضع و صُمم لينتج طريقة اتصال محددة بين برامج الجهاز الخادم و العميل Client-Server-Applications على بروتوكولات TCP و UDP لكي يؤمن الاتصال بين الأجهزة المستخدمة لتلك البروتوكولات .....(يكمل)

يحتوي الـ SOCKS على المحتويات التالية :

- ✓ SOCKS server : و اللذي يعمل على أي بيئة أساسها بيئة UNIX .
- ✓ SOCKS client library : و اللتي تعمل على الأجهزة اللتي في الشبكة الداخلية المحمية بالفايروول .
- ✓ SOCKS-ified : و هي عبارة عن التطبيقات اللتي يتداولها أجهزة العملاء مثل FTP,TELNET .
- ~ عندما ينوي العميل المعتمد على بروتوكول TCP (TCP-based client) فتح إتصال جديد بينه و بين جهاز أخر يمكن الوصول إليه فقط عن طريق الفايروول فإنه يجب فتح إتصال من بروتوكول الTCP و بتحديد Port له في الـ SOCKS server .
- ~ إن منفذ (port) خدمة الـ SOCKS في الاتصال عن طريق بروتوكول TCP هو منفذ رقم1080
- ~ إذا كان طلب العميل مقبول ، فإن العميل يدخل في مفاوضة لإتمام المصادقة بينه و بين الخادم على طريقة خروجه إلى العالم الخارجي ، ثم بعد ذلك يتم الإتصال .
- ~ تتم نفس الخطوات السابقة على بروتوكول UDP .

سنتكلم الأن عن نقطة أخرى متعلقة بموضعنا ألا و هو ال Bastion Host .

ما هو الـ Bastion Host ؟

هو نظام يتم تعريفه من مدير نظام الفايروول على أنه نقطة حرجة و خطيرة في الشبكة و اللتي تحتاج إلى حماية أكثر من بين نقاط الشبكة كلها . إن الBastion Host يخدم كمنصة عمل (Platform) لل Application-Level أو Circuit-Level gateway . هناك خصائص رئيسية لل bastion host و هي :

- ✓ Bastion Host Hardware منصة تعمل على إصدارة من نظام تشغيل يستطيع أن يلبي إحتياجاتها مثل ASA و PIX .
- ✓ لا أحد يستطيع تثبيت و تشغيل الخدمات عليها إلا مدير الشبكة و اللتي تتضمن خدمات ال Proxy و البروتوكولات اللتي تعمل كتطبيقات و غيرها مثل SMTP, FTP, Telnet وأيضا DNS و أيضا يتولى المصادقة في هذه الخدمات كلها وغيرها .
- ✓ إن مستخدمين ال Proxy يحتاجون مصادقة أكثر لكي يسمح لهم باستخدامه بالإضافة إلى أن كل Proxy server يحتاج أيضا مصادقة قبل السماح للمستخدمين باستخدامه .
- ✓ تستطيع أيضان أن تحدد نوع أنظمة التشغيل اللتي تعمل و تقوم بالمصادقة معه ، و هذا يعني تحديد الأوامر و الخدمات اللتي تعمل مع البروتوكولات عبر الشبكة .
- ✓ يستطيع البروكسي جمع و تتبع و مراقبة البيانات و تسجيلها .
- ✓ إن برامج البروكسي اللتي توضع و تنصب على سيفراتها بسيطه و خفيفة علا النظام و سهلة في التعامل معها .
- ✓ تستطيع Proxy Servers أن ترتبط ببعضها البعض و لا يؤثر ذلك على كفاءتها و عن حاجة مدير الشبكة لإضافة (سماح- منع) اي خدمة جديدة فإنه يعتبر أمرا سهل جدا حتى و إن وجدت نقطة حرجه Bastion Host .

- ✓ إن استخدام البروكسي في الشبكة بالنسبه للمستخدمين لا يعطيهم أي صلاحيات في منطقة ال Bastion Host .

من أمثلة الفايروولات :

Linux << IPtables

Cisco << PIX

Cisco << ASA

Microsoft << ISA

Juniper << Juniper firewall

اسم الكاتب : KING SABRI

الموقع: king-sabri.net